UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/713,980 | 11/14/2003 | Brian D. Swander | 14917.0474US01 | 3167 |

27488 7590 09/02/2008
MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

| EXAMINER | |
|---|---|
| PALIWAL, YOGESH | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/02/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/713,980 | SWANDER ET AL. | |
| | Examiner | Art Unit | |
| | YOGESH PALIWAL | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *26 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-9,18-22,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 18-22 and 26-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

- Applicant's submission for RCE filed on May 15, 2008 has been entered.
- Applicant has amended (amendments submitted with RCE) claims 1, 3, 5-8, 18, 20-22 and 26-27 and further amended (with submission of supplemental amendment filed on June 26, 2008) claims 1, 18, 26 and 27. Currently claims 1-9, 18-22 and 26-27 are pending in this application.

### *Response to Amendment*

1. Applicant has amended all independent claims which necessitated new grounds of rejections.

### *Response to Arguments*

2. Applicant's arguments with respect to claims 1, 18, 26 and 27 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent

granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6, 8-9, 18-21 and 26-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Zhou (J. Zhou, "Further Analysis of the Internet Key Exchange Protocol", Computer Communications, Vol. 23, Issue 17: Pages: 1606-1612, Publication: 2000), hereinafter "Zhou".

Regarding **Claims 1 and 18**, Zhou discloses a communication system in for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method including a plurality of modes, comprising:

conducting an internet key management and exchange protocol (IKE) main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol (see, Page 1607, Section 2.2, "Main mode protocol");

conducting an internet key management and exchange protocol (IKE) quick mode negotiation for deriving a set of keys usable with the security protocol (see, Page 1608, Section 2.4, "Quick mode protocol");

wherein at least one message that comprises at least part of the IKE quick mode negotiation is sent during the IKE main mode negotiation (see, Page 1607, Section 2.2, messages 3 and 4 of the main mode protocol) and a quick mode pseudo random number is exchanged between the responder and the initiator before completion of the IKE main mode negotiation (see, Page 1607, Section 2.2, messages 3 and 4 of the main mode protocol, $N_i$ and $N_r$); and

wherein a protocol security process establishes inbound and outbound protocol security associations (see Pages 1606 and 1607, Section 2.1, "Security association").

Regarding **Claims 2 and 19**, the rejection of claims 1 and 18 is incorporated and Zhou further discloses conducting a first user mode for authenticating a first user associated with the initiator or responder (see, Page 1607, 2nd Column, "Until the end of Step 4…generic payload heads").

Regarding **Claims 3 and 20**, the rejection of claims 2 and 19 is incorporated and Zhou further discloses wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the IKE main mode negotiation (see, Page 1607, 2nd Column, "Until the end of Step 4…generic payload heads").

Regarding **Claim 4**, the rejection of claim 2 is incorporated and Zhou further discloses conducting a second user mode for authenticating a second user associated with the initiator or the responder (see, Page 1607, 2nd Column, "Until the end of Step 4…generic payload heads").

Regarding **Claim 5**, the rejection of claim 1 is incorporated and Zhou further discloses wherein the IKE main mode comprises:

sending, from the initiator to the responder, a set of proposed security parameters and authentication data; selecting, by the responder, the set of security parameters from the set of proposed security parameters; and sending the set of security parameters from the responder to the initiator (see, Page 1607, Section 2.2, "Main mode protocol").

Regarding **Claims 6 and 21**, the rejection of claims 1 and 18 is incorporated and Zhou further discloses wherein the initiator identifies a public key of the responder prior to the IKE main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key (see, Page 1607, 2nd Column, "$g^x_i$ and $g^x_r$ are Diffie-Hellman...").

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Zhou further discloses exchanging Diffie Hellman key data between the initiator and the responder during IKE main mode for deriving keys for use with an encryption algorithm (see Page 1607, Section 2.2, 1st paragraph).

Regarding **Claim 9**, the rejection of claim 1 is incorporated and Zhou further discloses exchanging a pair of notify payloads between the initiator and the responder; wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations (see, Page 1607, Section 2.2, Messages 1 and 2).

Regarding **Claim 26**, Zhou discloses a method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

sending, from the initiator, a first message, wherein the first message comprises part of an internet key management and exchange protocol (IKE) main mode negotiation and the IKE main mode negotiation comprises establishing the secure path and selecting a set of security parameters including a security protocol (see, Page 1607, Section 2.2, Message 1);

receiving, at the initiator, a second message (see, Page 1607, Section 2.2, Message 4), wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation (4th message comprises $HDR_4$ and $KE_r$ which are part of the IKE main mode negotiation and also comprises $N_r$ which is used to derive set of keys of quick mode see, Page 1608, 4th paragraph, therefore, $N_r$ can be interpreted as a part of the IKE quick mode negotiation) and the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol (see, Page 1607, Section 2.2, SKEYID_d, DKEYID_a and SKEYID_e) and wherein the second message includes a quick mode pseudo random number (see, page 1607, section 2.2, 4th message comprises $N_r$);

sending, from the initiator, a third message after receiving the second message, wherein the third message comprises at least part of the IKE main mode negotiation (see, Page 1607, Section 2.2, 5th message); and

wherein a protocol security process establishes inbound and outbound protocol security associations at the initiator (see Pages 1606 and 1607, Section 2.1, "Security association").

Regarding **Claim 27**, Zhou discloses a method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

receiving, at the responder, a first message, wherein the first message comprises at least part of an internet key management and exchange protocol (IKE) main mode

negotiation and the IKE main mode negotiation comprises establishing the secure path and selecting a set of security parameters including a security protocol (see, Page 1607, Section 2.2, Message 1);

sending, from the responder, a second message (see, Page 1607, Section 2.2, Message 4), wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation (4th message comprises HDR4 and KEr which are part of the IKE main mode negotiation and also comprises Nr which is used to derive set of keys of quick mode see, Page 1608, 4th paragraph, therefore, Nr can be interpreted as a part of the IKE quick mode negotiation) and wherein the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol (see, Page 1607, Section 2.2, SKEYID_d, DKEYID_a and SKEYID_e) and wherein the second message includes a quick mode pseudo random number (see, page 1607, section 2.2, 4th message comprises Nr); and

wherein a protocol security process establishes inbound and outbound protocol security associations (see Pages 1606 and 1607, Section 2.1, "Security association").

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhou in view of Inoue et al. (US 6,170,057 B1), hereinafter "Inoue".

Regarding **Claims 7 and 22**, the rejection of claim 1 is incorporated and Zhou does not disclose the mode wherein a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator. The group advertisement corresponds to the security parameters of the remote network gateway.

Inoue discloses a system wherein a mode which comprises sending a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator (column 7 lines 20-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Zhou. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135